



Los 10 consejos más importantes para protegerse contra el robo de identidad

Un ladrón de identidad es una persona que obtiene su información personal y la usa sin su conocimiento. El ladrón puede endeudarse o hasta cometer delitos en su nombre. Los siguientes consejos pueden reducir su riesgo de ser víctima.

1. Proteja su número del Seguro Social.

No lleve su tarjeta del Seguro Social en su billetera o cartera. Si su plan de salud (excepto Medicare) u otra tarjeta usa su número del Seguro Social, pida que la compañía le dé otro número. Para obtener más información, vea la *Hoja 4 de información al consumidor: Su número del Seguro Social: Cómo controlar la clave del robo de identidad* en nuestra página Web sobre números del Seguro Social.

2. Combata la “pesca cibernética” – no muerda el anzuelo.

Los estafadores tratan de atrapar a sus víctimas haciendo “pesca cibernética”, simulando ser bancos, empresas o dependencias gubernamentales. Lo hacen por teléfono, por correo electrónico o correo normal. No proporcione información personal a menos que sea usted el que hace el contacto. No responda a una solicitud para verificar su número de cuenta o contraseña. Las compañías legítimas no solicitan este tipo de información de esta manera.

3. Evite que descubran su identidad en la basura.

Triture o rompa documentos que contengan información personal antes de botarlos a la basura. Destruya las ofertas de tarjetas de crédito y “cheques de conveniencia” que no vaya a usar.

4. Controle su información financiera personal.

La ley de California exige que su banco y otras compañías de servicios financieros obtengan su permiso antes de compartir su información financiera personal con otras empresas. También tiene el derecho de limitar la cantidad de información personal que puedan compartir con sus filiales de servicios financieros. Para obtener más información, vea la *Hoja 2 de información al consumidor: Sus derechos a la privacidad financiera*.

5. Proteja su computadora de virus y espías.

Proteja la información personal que se encuentre en la computadora de su hogar. Use contraseñas robustas: por lo menos de ocho caracteres, incluyendo una combinación de letras, números y símbolos,



fáciles de recordar para usted, pero difíciles de adivinar para los demás. Use software de protección cortafuegos (*firewall*), contra virus y spyware, y actualícelo periódicamente.

Tenga mucho cuidado y evite el software espía (*spyware*). Descargue software gratis sólo de sitios Web que conozca y sean de confianza. No instale software sin saber de qué se trata. Ajuste la seguridad de su navegador de Internet por lo menos a nivel “medio”. No haga clic en ventanas emergentes ni en correo electrónico no solicitado (*spam*). Vea nuestra *Hoja 12 de información al consumidor: Proteja su computadora contra virus, piratas informáticos y espías*.

6. Haga clic con precaución.

Cuando haga compras en línea, verifique el sitio Web antes de ingresar su número de tarjeta de crédito u otra información personal. Lea las normas de privacidad y fíjese si hay una opción para no tener que compartir información. (Si no hay normas de privacidad publicadas, ¡tenga cuidado! Haga sus compras en otro lado). Sólo ingrese información personal en páginas Web seguras cuyas direcciones empiecen con “https” y el símbolo del candado al pie de la ventana del navegador. Éstos son signos que indican que su información será encriptada o cifrada, protegiéndola de los piratas informáticos. Vea nuestra *Hoja 6 de información al consumidor: Cómo leer normas de privacidad*.

7. Verifique sus facturas y resúmenes bancarios.

Abra sus facturas de tarjetas de crédito y resúmenes bancarios de inmediato. Examínelos cuidadosamente para ver si hay cargos o desembolsos no autorizados e infórmelos inmediatamente. Si las facturas no llegan a tiempo, llame para averiguar qué pasó. Es posible que alguien haya cambiado su información de contacto para ocultar cargos fraudulentos.

8. Impida que le envíen ofertas de crédito “preaprobadas”.

Impida que le envíen la mayoría de las ofertas de crédito “preaprobadas” (aprobadas de antemano). Son un blanco tentador para los ladrones de identidad que roban correspondencia. Pida que eliminen su nombre de las listas de mercadeo de las agencias de crédito. Llame al teléfono sin cargo 1-888-5OPTOUT (888-567-8688). O visite www.optoutprescreen.com y elimine su propio nombre de las listas.

9. Haga preguntas.

Cuando le soliciten información personal que le parezca inapropiada para la transacción que está realizando, pregunte por qué la solicitan. Pregunte cómo se va a usar la información y con quién se va a compartir. Pregunte cómo será protegida. Explique que está preocupado por el robo de identidad. Si no está satisfecho con las respuestas, considere la posibilidad de ir a otro lado.

10. Consulte sus informes de crédito, gratis.

Una de las mejores maneras de protegerse contra robo de identidad es vigilando su historial de crédito. Puede obtener un informe de crédito gratis todos los años de cada una de las tres agencias nacionales de crédito: Equifax, Experian y TransUnion. Solicite los tres informes al mismo tiempo, o conviértase en su



propio servicio de vigilancia de crédito sin cargo. Simplemente solicite sus informes en forma espaciada, encargándolos de una agencia distinta cada cuatro meses. (Los servicios más comprensivos de vigilancia de crédito de las agencias de crédito cuestan de \$44 a más de \$100 por año). Encargue sus informes de crédito anuales llamando al teléfono sin cargo 1-877-322-8228 ó en línea en www.annualcreditreport.com. También puede enviar un pedido de informe por correo. Vea nuestra *Hoja 11 de información al consumidor: Cómo encargar sus informes de crédito gratuitos*.

Esta hoja se proporciona con fines informativos y no debe interpretarse como asesoramiento legal ni como la política del Estado de California. Si desea obtener asesoramiento sobre un caso en particular, debe consultar con un abogado u otro experto. Esta hoja de información se puede copiar, siempre y cuando (1) no se cambie ni se desvirtúe el significado del texto copiado, (2) se dé crédito a la Oficina de Protección de Privacidad de California y (3) todas las copias se distribuyan sin cargo.